REMARKS

In response to the Office Action dated May 3, 2002, claim 16 is amended, and claims 1-6 and 12-15are canceled. Claims 2-11 and 16-19 are now active in this application. No new matter has been added.

REJECTION OF CLAIMS UNDER 35 U.S.C. §102

Claims 1-19 stand rejected under 35 U.S.C. §102(3) as being anticipated by Hayakawa.

Claims 1-29 stand rejected under 35 U.S.C. §102(e) as being anticipated by Judd et al. (hereinafter, Judd).

The rejection of claims 7-11 and 16-19 is respectfully traversed.

Anticipation, under 35 U.S.C. § 102, requires that each element of the claim in issue be found, either expressly described or under principles of inherency, in a single prior art reference. ***Kalman v. Kimberly-Clark Corp.***, 713 F.2d 760, 218 USPQ 781 (Fed. Cir. 1983).

Claim 7 recites:

> A method of transmitting a data packet received by a ***repeater*** from a transmitting network node on a corresponding repeater port, the method comprising:
>
> identifying one of a plurality of ***repeater*** ports serving a destination network node based on a destination address in the data packet;
>
> transmitting the data packet on the one ***repeater*** port serving the destination network node by concurrently asserting a transmit enable signal on a corresponding media independent interface; and
>
> corrupting transmission of the data packet on other ***repeater*** ports by concurrently asserting a transmit error signal and deasserting the transmit enable signal on the media independent interfaces corresponding to the other ***repeater*** ports.

Claim 16 recites:

> A ***repeater*** system comprising:
> ***repeater*** ports for communication with respective network nodes via respective ***repeater*** media independent interfaces; and
> a ***repeater*** core comprising:
> (1) a table for identifying each network node by its corresponding destination address and the corresponding ***repeater*** port, and
> (2) a security circuit for transmitting a data packet on an identified one of the ***repeater*** ports corresponding to the network node having the destination address specified in the data packet, the security circuit corrupting transmission of the data packet on other of the network ports by concurrently asserting a transmit error signal and deasserting a transmit enable signal on the respective media independent interfaces.

As a first issue, independent claims 7 and 16 each require that there be a repeater with repeater ports. Neither Hayakawa nor Judd disclose a repeater. Consequently, anticipation is not established as each element/step of each of claims 7 and 16 is/are not found in Hayakawa or Judd.

Secondly, what is being done in Hayakawa and Judd is substantially different from what is being done in the present invention as represented by independent claims 7 and 16. More specifically, the present invention addresses a problem of conventional repeaters where any network node can eavesdrop on all packets that are transmitted on the network, and hence, an unauthorized workstation may eavesdrop on all data packets by obtaining access to a repeater port. This problem is addressed in the present invention by an arrangement for secure repeater communications to network nodes where network data is transmitted for repeater ports serving the destination network node of a given data packet and by transmitting corrupted network data for repeater ports that do not serve the destination network node of the given data packet, without the unnecessary generation of symbol errors.

Hence, once a repeater core identifies a repeater port as corresponding to the network node having the destination address specified in the data packet, a security circuit transmits the data packet on the identified repeater port by asserting the transmit enable signal (TX_EN) for the corresponding network port concurrently with transmitting the transmit data on the signal path of a shared bus. In addition, the security circuit transmits corrupt data on repeater ports that correspond to network nodes that do not have the destination address specified in the data packet with concurrently asserting the transmit error signal (TX_ER) and deasserting the transmit enable signal (TX_EN) on the respective media independent interfaces.

Method claim 7 and combination claim 16 each require these specific features.

As noted above, what is being done in Hayakawa and Judd is substantially different from what is being done in the present invention. Both Hayakawa and Judd are concerned with addressing transmission errors, which the present invention is not. More Specifically, in Hayakawa, when a reception node (of a receiving network device) determines that there has been a reception error, the reception node issues a re-transmission request of data to the transmitting node (of the distinct transmitting network device). If reception error occurs only in some receiving nodes, then only the nodes at which the reception error occurred issues the re-transmission request to the transmitting node (of the separate and distinct transmitting network device). In Judd, an error recovery system/method is disclosed. More specifically, Judd is concerned with recovering from errors occurring during transmission of data between (distinct network) nodes.

In the operations described in each reference, data is being transmitted between ports of distinct network devices. The references are not concerned with what is being transmitting from different ports of a ***single*** network device. More specifically, neither reference discloses or suggests a (repeater) port (of a single repeater device) corresponding to the network node having the destination address specified in a (received) data packet from which the (received valid) data packet is transmitted to the specified address, and (at least one) another port (of the single repeater device) corresponding to a network node that does not have the destination address specified in a (received) data packet from which corrupted data is transmitted.

Thus, claims 7-11 and 16-17 are patentable over Hayakawa and Judd as the Examiner has not established a prima facie case of anticipation. Consequently, it is respectfully requested that the rejection of claims 7-11 and 16-17 be withdrawn, and that these claims be allowed.

To expedite prosecution, claim 16 is amended to clarify that "the security circuit corrupting transmission of the data packet on other of the ***repeater*** ports corresponding to network nodes not having the destination address specified in the data packet ..."

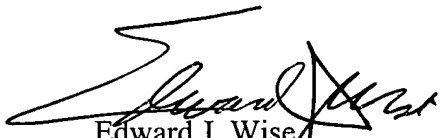
CONCLUSION

Accordingly, it is urged that the application, as now amended, is in condition for allowance, an indication of which is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, Examiner is requested to call Applicants' attorney at the telephone number shown below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Edward J. Wise
Registration No. 34,523

600 13th Street, N.W.
Washington, DC 20005-3096
(202)756-8000 EJW:khb
Facsimile: (202)756-8087
Date: June 12, 2002

VERSION WITH MARKINGS SHOWING CHANGES MADE

IN THE SPECIFICATION

Page 1, amend the paragraph beginning at line 19 as follows:

Figure 1 is a diagram illustrating a conventional repeater network. The network 10 includes a repeater 12 configured for transmitting a data packet received on an input port to the other ports for reception by the respective network nodes 14. For example, assume that node (i.e., workstation) 14a transmits a data packet via the network medium 16. The transmitted data packet is received by a physical layer transceiver (PHY) 20a which recovers the digital data from the transmitted analog signal. As recognized in the art, the PHY transceiver 20a may be a 100 Base-TX IEEE standard 802.3u receiver, configured for receiving a 3-level MLT-3 encoded analog signal at a 125 Megabit per second rate, and configured for output of the transmit data as nibble-wide (4 bits) or byte-wide transmit data (TXD) to the MII 18 between the PHY 18 and the repeater 12. The repeater 12, upon receiving the transmit data from the PHY transceiver [28a] 20a, retransmits the transmit data to all the other ports for transmission by the other PHY transceivers (e.g., [28b, 28c, and 28d] 20b, 20c, and 20d). The network stations 14 of the other ports will ignore the packet unless the destination address of the packet matches the network stations own address. One problem with the arrangement is that any network node can eavesdrop on all packets that are transmitted on the network. Hence, an unauthorized workstation 14e may eavesdrop on all data packets by obtaining access to a repeater port.

Page 7, amend the paragraph beginning at line 19 as follows:

As shown in Figure 4, the state machine and the detection circuit 50 begins in the idle state 60, where the physical layer transceiver 36 receives idle symbols from the corresponding MII 40 and with both the transmit enable and transmit error signals equal to 0. Upon initial transmission of the data packet by the repeater core 32, the security circuitry 46 asserts the transmits enable (TX_EN) signal (TX_EN=1) until the entire destination address can be encoded [1,0]. As shown in Figure [6] 4, the transmit enable is asserted upon detection of a preamble (e.g., following detection of J and K symbols in sequence). The transmit enable signal is asserted on all repeater ports 34 until the destination address (DA) of the data packet 58 can be decoded. In response to detecting assertion of the transmit enable signal (TX_EN=1) and deassertion of the transmit error signal (TX_ER=0), the detection circuit 50 moves from state 60 to state 62 during the next clock cycle. If during state 62 the transmit enable signal is deasserted (TX_EN=0) or transmit error is asserted (TX_ER=1), the detection circuit returns to state 60. However, if the transmit enable signal is asserted concurrent with deassertion of the transmit error signal for another clock cycle, the detection circuit 50 moves to state 64. The detection circuit 50 remains in state 64 until deassertion of both the transmit enable and transmit errors signals [0,0] (e.g., end of transmission), a detected error condition by concurrent assertion of both the transmit enable and transmit errors signals [1,1], or upon detection of a corruption state. The detection circuit 50 detects at state 64 the occurrence of a corruption by the concurrent assertion of the transmit error signal and deassertion of the transmit enable signal, causing the detection circuit 52 to move to the jam 1 state 66.

IN THE CLAIMS:

Please amend the claims as follows:

16. (Amended) A repeater system comprising:

repeater ports for communication with respective network nodes via respective repeater media independent interfaces; and

a repeater core comprising:

(1) a table for identifying each network node by its corresponding destination address and the corresponding repeater port, and

(2) a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet, the security circuit corrupting transmission of the data packet on other of the [network] repeater ports corresponding to network nodes not having the destination address specified in the data packet by concurrently asserting a transmit error signal and deasserting a transmit enable signal on the respective media independent interfaces.